A comprehensive authentication and supervision architecture for networked multimedia systems

S.M.Furnell[†]*, H.M.Illingworth*[†]*, S.K.Katsikas*[‡]*, P.L.Reynolds*[†] *and P.W.Sanders*[†]

[†] *Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, United Kingdom.*

[‡] *Research Unit, University of the Aegean, 30 Voulgaroktonou Street, Athens, Greece*

E-mail : stevef@pbs.plym.ac.uk, heleni@pbs.plym.ac.uk

Abstract

The paper identifies the need for improved user authentication and supervision techniques within local security domains. Whilst there are now appropriate standards for the security of inter-domain operations, authentication of the users within them is often still reliant upon measures that are open to compromise and which provide no safeguard against system misuse.

The discussion presents an overview of various potential authentication and supervision techniques (largely based upon a combination of physiological and behavioural biometrics), discussing the relative advantages and disadvantages of each from an implementation perspective.

The discussion then proceeds to consider how these approaches may be integrated into a comprehensive architecture for user and system supervision entitled IMS (Intrusion Monitoring System). The conceptual approach of this system is described, with details of the functional modules involved and the intended operation of the monitoring process.

The paper concludes by considering how the supervision approach would be integrated into a wider security framework, involving inter-domain operation and Trusted Third Party (TTP) certification.

Keywords

Authentication, Intrusion Detection, Biometrics, Trusted Third Party.

1 INTRODUCTION

As information technology systems assume ever more importance in the successful operation of modern organisations and societies, so the need for adequate means of ensuring authorised and correct use of facilities within and between systems becomes increasingly essential. Methods exist to enable the authentication of communicating parties between domains, along with the confidentiality, integrity and non-repudiation of transmitted data / messages (CCITT 1989). However, trust and certification between domains is only appropriate if adequate authentication can be performed within the individual systems involved.

In most traditional systems the principal means of user authentication is via the password. Whilst relatively acceptable in terms of ease of use and implementation, the weaknesses of passwords (e.g. vulnerability to compromise through poor selection and infrequent change) are well documented (Jobusch and Oldehoeft 1989). Even smart cards cannot provide a guarantee of user authentication, and systems may still be vulnerable to compromise in some circumstances (e.g. if the legitimate user leaves an active session unattended). In addition, smart cards do not provide any inherent protection against system misuse by authorised users. Finally, such an approach may be considered impractical as a compulsory measure due to the immediate financial burden associated with the installation of card readers and issuing of cards. As such, there is a need for other approaches to authentication, which do not sacrifice advantages such as ease of use.

2 APPROACHES TO AUTHENTICATION AND SUPERVISION

A number of methods may be appropriate to the above requirements, based upon a combination of physiological and behavioural biometric techniques. The principles behind these are described in the paragraphs that follow, along with an indication of their effectiveness where possible (note: effectiveness in this context relates to the False Acceptance and False Rejection Rates - FAR and FRR - associated with each measure). All of the characteristics would be assessed and held in a *profile* for each legitimate system user within the monitored domain.

- *Face Recognition*
  Face recognition is a physiological biometric technique that most people use every day in order to recognise others. Everyone has unique facial characteristics that distinguish them from others. Research into this area has proven to be successful, with authentication judgements made within 1.5 seconds and an error rate of 2.5% (Secure Computing 1995). There are several different methods for achieving this, including pattern recognition, neural networks, von der Malsburg's graph matching and isodensity maps.

  Additional hardware and software is required to enable face recognition to be used. A video camera with video-capture board, as well as appropriate software will be needed for each workstation to be monitored. At the present time, this would prove to be an expensive exercise, although with multimedia and video-conferencing becoming increasingly common, costs are likely to reduce.

  With a small camera positioned on a monitor, users could be monitored continuously or perhaps periodically, to verify that the user logged-in is the legitimate owner of the account. This would provide stronger authentication than the current initial login methods.

- *Voice Recognition*

  Voice authentication techniques are already being used for physical access control, access to long distance telephone lines and voicemail. Voice authentication differs from speech recognition in that it tries to distinguish one person from another. It is not concerned with the words spoken but with their spectral content. On the other hand, speech recognition distinguishes one word from another and attempts to ignore speech characteristics.

  A typical system works by recording and storing the user's voiceprint. Once this has been done, a user speaks a password or phrase which is then compared to the stored voiceprint. If verified, the user gains access to the system. Some more advanced systems have the capability of adaptively updating the voiceprint records. This has the advantage of tracking any changes to a user's voice.

  As with face recognition, additional hardware and software will be required although both the complexity and cost of the hardware is much lower. This technique would most commonly find a role as an initial password verification tool and has limited potential for continuous monitoring. However, wider use would be possible if a subject routinely uses dictation tools or similar.

  Typical error rates for this technique are claimed to be an FRR of 1% and an FAR of as low as 0.0001% (Cope 1990).
- *Keystroke Analysis*

  Keystroke analysis refers to the verification of user identity through the monitoring and assessment of typing characteristics, based on the assumption that the difference in style between the legitimate user and an impostor is likely to be very marked. A number of factors may provide a basis for discrimination, including inter-keystroke times, keypress duration and typing error frequency.

  Keystroke analysis may be implemented in two ways - termed the static and dynamic verification strategies. In the static scenario, authentication is based upon entry of a known text string, such as a username and password. The information would be entered as usual, but the system would also analyse the way in which it was typed. By contrast, dynamic analysis is based upon any arbitrary keyboard input, allowing greater scope for continuous user supervision. Both approaches have been subject to a number of experimental studies and typical measures of effectiveness are 0.5% FAR and 3.1% FRR for the static approach (Bleha et al. 1990) and 15% FAR and 0% FRR for the dynamic approach (Furnell et al. 1996).
- *Mouse Dynamics*

  Mouse dynamics is a new area of research which involves monitoring characteristics of mouse usage. Current research is looking at measurements of speed and acceleration in order to distinguish one person from another. These measurements may be taken without the need for any physical changes to the current mouse design and require only minimal software changes. These measurements can be taken when a user makes a selection from a pull-down menu, moves the pointer or uses the mouse in other ways.

  Mouse dynamics monitoring is limited to Graphical User Interface (GUI) environments where mouse usage is greatest. A recent exploratory study gave an average error (FAR/FRR combined) of between 14% and 39% (Barrelle et al. 1996), indicating that the technique requires further refinement before it is comparable with some of the other approaches.
- *Behaviour monitoring*

This technique is based upon the monitoring of the users interaction with the system. It is founded on the premise that everyone has their own characteristic or preferred way of doing things when using a system. As such, behaviour monitoring may actually encompass a number of further profiled characteristics, some examples of which are given in Table 1 below.

Table 1 Potential characteristics for behavioural profiling

Characteristic	*Description*
Access Time	Time(s) between which subjects typically access IT systems. In some cases there may be a detectable correlation between access time and application usage, allowing a continuous measure.
Access Location	May be approached from two perspectives : monitoring the location(s) from which subjects typically access IT systems OR monitoring which subjects normally access from any given terminal / port.
OS Command Usage	Type and frequency of operating system commands used.
Application Use	Type and frequency of application systems used.
User Interaction	Monitoring of the method(s) by which a subject commonly interacts with the system / applications (e.g. keyboard or mouse, commands or menus).
Resource Usage	Statistics of typical usage of system resources (e.g. CPU, memory, disk) associated with each subject.
Access Violations	Tracking of the number of access violations (e.g. to files, data, applications, devices) made by a user / process during a session.

Individual behaviour profiles would need to be developed using data collected over a reasonably long time period, in order to establish what constitutes "normal" behaviour for each legitimate user.

Effectiveness in this case would depend upon the exact combination of characteristics being monitored and, as such, it is not possible to give a general figure. The approach is a key element of a number of intrusion detection systems, including IDES (Lunt 1990) and SecureNet (Androutsopoulos et al. 1994).

It is acknowledged that there are a number of other biometric authentication measures that may also be technically feasible, including fingerprint analysis, hand geometry or signature recognition. However, these are considered to offer less potential for transparent or continuous integration into the supervision system, given that they require more specific actions on the part of the user. In addition, the required hardware in each of these cases would not be a likely "standard" feature of any system (multimedia or otherwise) and would, therefore, represent an additional expense. The perceived advantages and disadvantages of the chosen approaches are presented in Table 2.

Table 2 Advantages and disadvantages of authentication / supervision approaches

Method	*Advantages*	*Disadvantages*

Method	*Advantages*	*Disadvantages*
Face Recognition	• Low error rates • Continuous monitoring	• Requires extra hardware • Complexity and cost • Restricted number of users due to database size and complexity • Will not detect insider attacks
Voice Recognition	• Low error rates • Most mature technology of the techniques discussed	• Requires extra hardware • Complex • Generally restricted to initial login • Will not detect insider attacks
Keystroke Analysis	• Continuous monitoring • Low cost • Works with existing systems requiring no extra hardware	• Experimental technology • Will not detect insider attacks • For continuous monitoring, can only be used in keyboard-intensive applications (e.g. word-processing)
Mouse Dynamics	• Continuous monitoring • Low cost • Works with existing systems requiring no extra hardware	• New technology • Will not detect insider attacks • For continuous monitoring, can only be used in GUI-based applications
Behaviour Monitoring	• Continuous monitoring • Detects insider attacks • Low cost • Works with existing systems requiring no extra hardware	• New technology

It is possible to categorise the techniques into different groups, according to the general strength and reliability of the authentication / supervision measures that they deliver. As such, they can be seen to reside at different "confidence levels", as illustrated in Figure 1 below (note that, for simplicity, the measures are split into just three levels, although there could conceivably be more in practice).

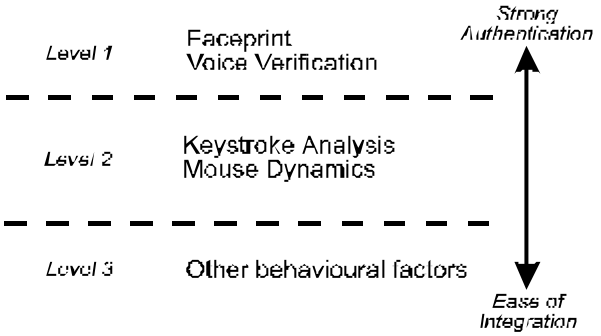

Figure 1 Comparison of the authentication / supervision measures.

As indicated in the figure, the strength of the measures in terms of their potential for accurate user authentication decreases as one moves down through the levels. However, other positive factors can

be cited, including the ease of practical implementation / integration into existing systems, the transparency of the measure, the potential to detect internal abusers and the financial viability.

It should also be noted that the "confidence level" attached to a particular technique need not be static, but could vary depending upon the usage context of the system. For example, in a word-processing context, keystroke analysis may be viewed as a high-confidence measure, whilst it would only qualify as a low-confidence measure (if at all) in a web browsing scenario.

It can be seen fom the above that whilst appropriate techniques have been developed and evaluated independently, the effectiveness of a composite approach has not yet been assessed and demonstrated in practice.

3 THE INTRUSION MONITORING SYSTEM (IMS) ARCHITECTURE

It is clear from the previous studies that none of the approaches identified can offer a guarantee of correct authentication in all cases. A means of combining the techniques into a comprehensive framework is, therefore, required such that other measures can compensate when one method is failing. For example, based upon the previous discussion of the "confidence levels" offered by different measures, it is possible to assess potential intrusion alerts according to all of the measures available at the time.

It is suggested that this combination of techniques should occur within the context of the supervision architecture specified for the Intrusion Monitoring System or IMS (Furnell 1995). This aims to provide a generic framework for user authentication and system intrusion detection, within which a number of technologies may be integrated.

At a high level the architecture is based upon the concept of a central monitoring Host which handles the authentication and supervision of a number of Client workstations. Both the Host and Client would be implemented in software, communicating over a standard network link (e.g. Internet / TCP/IP). The Host acts as the custodian of all user profiles and other security monitoring information, whilst the role of the Client(s) is to collect the required user / activity data and respond to any anomalies that are detected.

3.1 Generic intrusion indicators

In addition to the authentication and supervision techniques already identified, the IMS architecture also includes the concept of generic intrusion rules. These recognise that, in some cases, intrusions may be identified without requiring any historical knowledge of specific users behaviour. Rules may be incorporated to allow identification of specific events (or event series) that may be indicative of a security compromise (this will assist in the monitoring of the system state as well as user-related activity). Suitable rules could be based upon a number of factors, such as known intrusion scenarios / patterns of abuse ("attack signatures"), known weaknesses of the host system (e.g. operating system vulnerabilities), advice from security experts and audit trail analysis (Leipins and Vaccaro 1989).

The examination of known intrusion scenarios reveals several classes of event that should at least be regarded as "suspicious". A selection of potential examples are given in Table 3 below.

Table 3 Examples of generic intrusion indicators

Event	*Description*
Consecutive access violations	A significant number of failures during a session indicates that the user may be trying to access objects / resources for which he / she not authorised.
Account overuse	Simultaneous sessions utilising the same account may indicate that a hacker is using the system.
Out of hours access	Out of hours access (especially at night) may indicate unauthorised activity.
Use of inactive accounts	Sudden or unexpected activity on accounts that have been dormant for long periods may be worthy of investigation.
Extensive use of "help" systems	External penetrators may be unfamiliar with the system and its facilities and may refer to help systems frequently.

Whilst no single event may be conclusive of an intrusion, occurrences may be used to increase an IMS *alert status*. In this way, certain combinations of events may be identified that are much more significant than any event on its own. It should be noted that the larger the rule-base, the longer it will take for the system to search on each monitoring iteration (and, hence, the greater the processing overhead on the system). As such, it may be desirable to prioritise the rules in some way, enabling the monitoring system to minimise its effort.

3.2 IMS architecture overview

The full IMS architectural framework is illustrated in Figure 2 and described in the paragraphs that follow.

- *Anomaly Detector*
  The *Anomaly Detector* is responsible for analysing activities to identify suspected intrusions, using behaviour profiles and generic rules as the basis. The detector will maintain "alert status" values for each user session under supervision which would increase in response to either departures from the behaviour profiles or satisfaction of the intrusion rules. Reduction would occur after successful challenges or a sufficient period of normal activity to enable the apparent anomaly to be discounted.
- *Profile Refiner*
  There is a possibility that user activity may legitimately change over time. The *Profile Refiner* will utilise neural network techniques in order to identify suitable patterns of behaviour and then train the profiles, such that the effectiveness of monitoring can adapt and improve. The refinement process would only occur after the termination of non-anomalous sessions.

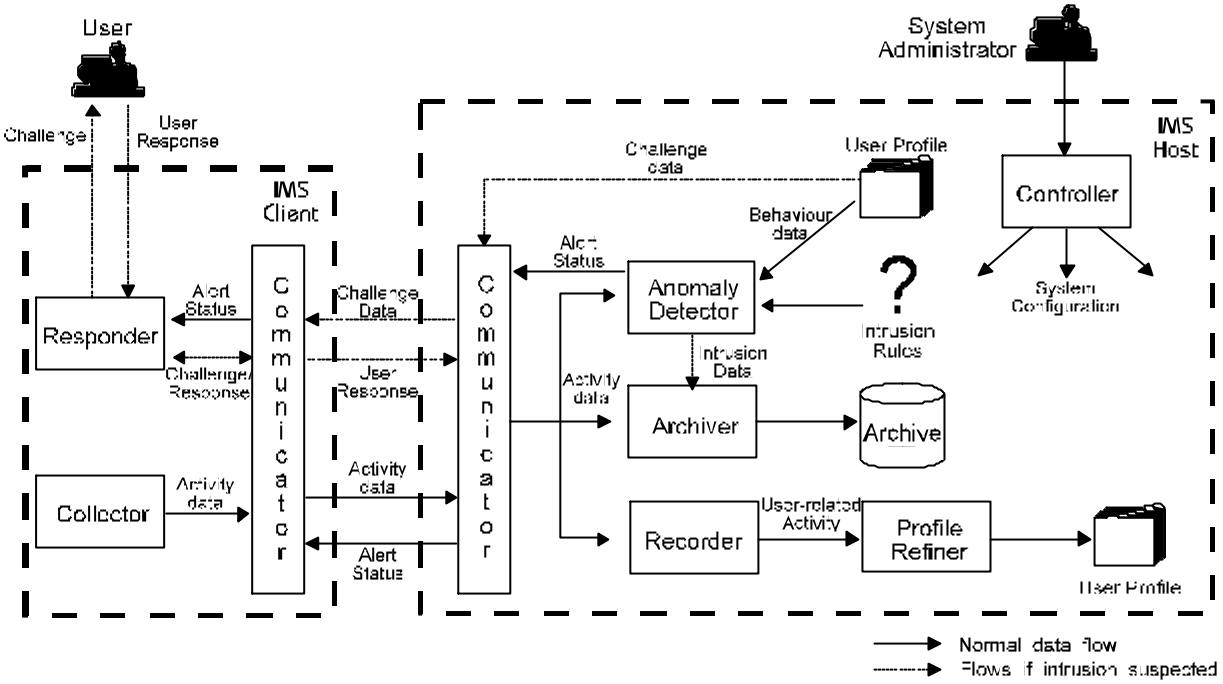

Figure 2 The IMS Architecture.

- *Recorder*
  This module handles the short-term storage of user-related activity data during an active session, which will then be utilised by the Profile Refiner upon session termination, provided that it was not considered anomalous.
- *Archiver*
  The *Archiver* module will collect information relating to IMS security-relevant events (e.g. login failures, intrusion alerts, challenges and the like) and maintain it in a long-term archive to provide a historical record of activities and suspected anomalies. The data would be stored irrespective of whether sessions or processes are considered to be anomalous at the time.
- *Collector*
  The Collector provides the interface between IMS and other system applications, and handles the task of obtaining any relevant information on user and system activity. The majority of collection activity would occur at the operating system level, with interrupts and service requests being intercepted / redirected such that key events are "visible" to the IMS supervision (e.g. keyboard actions, application execution etc.). In an operational scenario the information available to the *Collector* would be determined by the configuration of the user workstation and the current user activity. For example, faceprint recognition would not be possible if the workstation is not equipped with a camera. The resolution of data collection would be determined on the Host side by the System Administrator.
- *Responder*
  The *Responder* is ultimately responsible for dealing with any anomalies detected by the Host. Response would be based upon continuous monitoring of the alert status being sent by the Host, with increases being used to trigger appropriate actions. The response will vary depending upon the type and severity of the suspected intrusion. Appropriate options would include :
  - issuing of an explicit authentication challenge;

- recording of details in an intrusion log for later investigation;
- notification of the system manager (i.e. an intrusion alarm);
- phased reduction of permitted behaviour;
- locking of the intruder's terminal;
- termination (or suspension) of the anomalous session / process.

In the comprehensive framework suggested, the *Responder* would also be in control of the initial user identification and authentication process at login.

- *Communicator*

  The *Communicator* provides the communications interface between the Host and the Client systems. As such, the functionality of this module is duplicated at both ends. From the Client side, the *Communicator* would handle the transmission of the user and process data obtained by the *Collector*, whilst from the Host side it would be responsible for sending out the appropriate alert status to the Client(s) under supervision. The Client side would ensure that all information is presented to the Host in a standardised format, enabling operation within a heterogeneous operating environment.

- *Controller*

  The role of the *Controller* is to enable the System Administrator to configure the operation of the IMS system. On the Host side, this would apply to the Anomaly Detector (e.g. behaviour characteristics and intrusion rules to utilise), the *Profile Refiner* (e.g. frequency of refinement) and the *Archiver* (e.g. resolution of recording). With regard to the Client side, the configuration would apply to the *Collector* (e.g. the level of data collection) and the *Responder* (e.g. the appropriate response at each alert status level), with the settings being established at session initiation time. The *Controller* would also provide the link to facilities such as user profile management.

3.3 Comprehensive supervision strategy

It is suggested that comprehensive IMS intrusion detection could be based on a combination of several independent strategies, as shown in Figure 3.

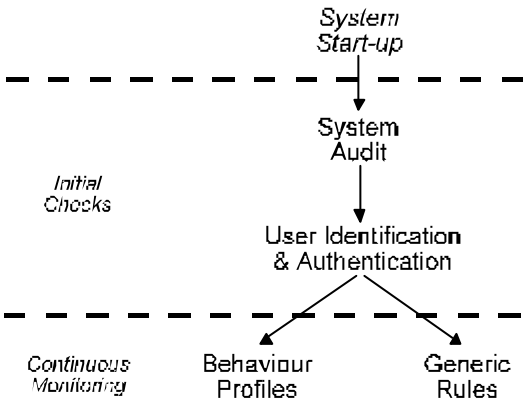

Figure 3 IMS user session supervision strategy.

The approach includes auditing of the local system configuration (which would incorporate virus scanning), initial user identification / authentication, on-going comparison of user activities against historical "behaviour profiles" and the use of generic rules to identify potentially anomalous system events.

The first task of IMS should be to ensure the integrity of the system upon which supervision is to be conducted. The local system should, therefore, be checked at user login or system start-up time. It is envisaged that certain configuration changes may have serious implications from a security standpoint (note: the configuration in this context encompasses factors relating to the system hardware, the operating system and any significant user defined settings). For example, they might be indicative of physical tampering with (or theft of) equipment, affect the compatibility and / or performance of existing applications (including the IMS supervisor itself), which could result in accidental security compromise or be indicative of a deliberate attempt to compromise security. As a countermeasure, relevant configuration data should be collected and stored by IMS, which may then be used for comparison against the system configuration on subsequent occasions to ensure that everything is still as expected.

Identification of the current user is necessary at the start of a session in order to enable the system to determine which profile should be used for supervision. In theory, the subsequent monitoring of behaviour could then act as the mechanism for authenticating the claimed identity. However, the inclusion of an initial authentication phase would allow the supervision to commence with an initial high confidence of user legitimacy. Such authentication (and the subsequent ongoing supervision) would be based upon one or more of the techniques described earlier, as appropriate to the Client system in question and the sensitivity of the user account.

4 SUPERVISION IN AN INTER-DOMAIN SCENARIO

Having established how the IMS architecture would function at a local level within an individual security domain, the paper will now briefly address the issue of how secure inter-domain operations would occur. In order to facilitate trusted wide-area communications between a number of independent, cooperating organisations, a widely recognised method is the use of a hierarchy of Trusted Third Party (TTP) systems (CCITT 1989). The TTPs role is basically that of a naming and certification authority, issuing trusted certificates of user credentials (principally their name and a public key) which can then be placed in a directory, making them accessible to other communicating parties. The certificates are signed by the TTPs at different levels of the hierarchy, thus enabling a trusted path extending to international levels. Such an arrangement is illustrated in Figure 4, showing two Universities as the local security domains.

The IMS Host would form part of the Security Management Centres (SMCs) within the individual domains, with Clients operating on the local workstations. The SMCs would also have the wider responsibility for ensuring the security of communications between the individual domains (Muftic et al. 1993). This would include the harmonisation of security services available within different domains and the subsequent mediation of data exchanges and messages.

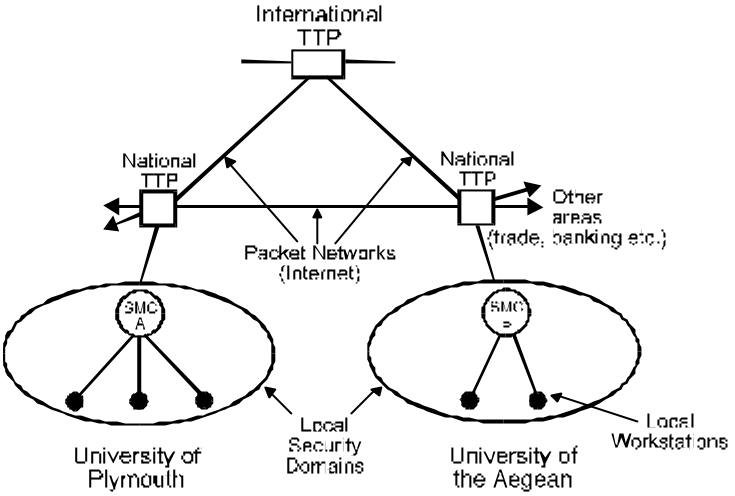

Figure 4 Interaction between secure domains.

The SMCs use of TTP-originated certificates would allow three main classes of service to be provided: confidentiality, integrity and non-repudiation. The need for authentication and supervision within the inter-domain context would occur if, for example, a user in domain A wished to remotely utilise a system in domain B. As such, there would be a requirement for interaction between the Hosts / SMCs in each domain in order to maintain the appropriate level of supervision. There would, in fact, be two potential approaches to monitoring in this scenario, as outlined below.

1. The authentication and supervision is still conducted locally by the IMS Host at SMC A. In this scenario, the inter-domain transmissions occurring as part of the user session would utilise the TTP certificates. This implies that SMC B trusts SMC A to perform correct authentication and that all necessary behaviour monitoring can be conducted within the users home domain.
2. The user profile is transferred to SMC B, such that user A's workstation becomes a remote Client to an alternative IMS Host. In this way, SMC B has more direct control over the supervision. This would be appropriate where more specific behaviour monitoring is required and also recognises the fact that the intrusion indicators in operation may differ between domains. In this scenario, one of the first messages would be a signed profile from domain A to domain B. During the subsequent session, various items of IMS-related data would be exchanged between the domains, using the TTP certificates as a means of securing the communication.

5 CONCLUSION

The paper has proposed a comprehensive monitoring framework which should be capable of offering a flexible security system, whilst maintaining a high degree of transparency and ease of use for the end user. The approach is considered to be particularly appropriate to modern multimedia systems, in which even the more advanced enabling technologies (e.g. image capture and audio processing facilities) are likely to be available. It is anticipated that the combination of authentication / supervision techniques will be effective in minimising both False Acceptance and False Rejection related errors. That said, however, it is also expected that the associated authentication tolerances, confidence levels and the like will require a reasonable degree of fine tuning in order to determine the

optimal configuration in practice. However, such a task could be performed automatically with an adaptive system, such that performance will be naturally inclined to improve over time.

A practical implementation of the IMS system is currently being realised for the Microsoft Windows environment and it is anticipated that a number of the techniques discussed in this paper will be incorporated. It is hoped that this will serve to provide proof of concept and validation of the approach in due course.

6 REFERENCES

Androutsopoulos, D.; Kaijser, P.; Katsikas, S.; Presttun, K.; Salmon, D. and Spirakis, P. (1994) Surveillance and Protection in IBC Management : The Applicability of Two RACE Security Projects - SecureNet II and SESAME, in *Proceedings of IS&N '94: 61-72*, Aachen, Germany.

Barrelle, K.; Laverty, W.; Henderson, R.; Gough, J.; Wagner, M. and Hiron, M. (1996) User verification through pointing characteristics: an exploration examination, *International Journal of Human-Computer Studies* **45**: 47-57.

Bleha, S.; Slivinsky, C. and Hussien, B. (1990) Computer-Access Security Systems Using Keystroke Dynamics, *Transactions on Pattern Analysis and Machine Intelligence* **12**, no. 12: 1217-1222.

CCITT (1989) Recommendation X.509 "The Directory-Authenticaion Framework", Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva.

Cope, B.J.B. (1990) Biometric systems for access control, *Electrotechnology*, April/May 1990: 71-74.

Furnell, S.M. (1995) Data Security in European Healthcare Information Systems, in PhD Thesis, University of Plymouth, UK.

Furnell, S.M.; Morrissey, J.P.; Sanders, P.W. and Stockel, C.T. (1996) Applications of keystroke analysis for improved login security and continuous user authentication, in *Proceedings of 12th International Conference on Information Security (IFIP SEC '96) : 283-294*, Samos.

Jobusch, D.L. and Oldehoeft, A.E. (1989) A Survey of Password Mechanisms : Part 1, *Computers & Security*, **8**, no. 7, 587-604.

Leipins, G.E; and Vaccaro, H.S. (1989) Anomaly Detection: Purpose and Framework, in *Proceedings of the 12th National Computer Security Conference : 495-504*, USA.

Lunt, T.F. (1990) IDES: An Intelligent System for Detecting Intruders, in *Proceedings of the Symposium : Computer Security, Threat and Countermeasures*, Rome, Italy.

Muftic, S; Patel, A.; Sanders, P.; Colon, R.; Heijnsdijk, J. and Pulkkinen, U. (1993) Security Architecture for Open Distributed Systems, *Wiley Professional Computing*, John Wiley & Sons Ltd, Chichester, England.

Secure Computing. (1995) Body Check - Biometrics Review, *Secure Computing*, July 1995: 30-39.